ANALISIS KEBUTUHAN SENJATA SIBER DALAM MENINGKATAN PERTAHANAN INDONESIA DI ERA PEPERANGAN SIBER

REQUIREMENT ANALYSIS OF CYBER-WEAPON TO IMPROVE INDONESIA DEFENSE IN CYBER-WARFARE ERA

Sri Hidayati[1], Rudi A.G. Gultom[2]
Program Studi Teknologi Persenjataan, Universitas Pertahanan

Abstrak- Serangan melalui dunia maya tanpa harus menghadirkan kekuatan militer secara fisik telah menjadi trend baru dalam perang modern di abad 21. Melalui *cyber attack,* sebuah negara dapat menciptakan dampak kerusakan yang meluas di negara lawannya, seperti melumpuhkan sistem kontrol dan kendali peralatan militer maupun sistem infrastruktur kritis lainnya. Beberapa negara maju telah membangun dan mempersiapkan organisasi pertahanan siber. Negara-negara tersebut telah memiliki militer modern yang disiapkan untuk menggunakan dunia maya sebagai medan pertempuran paralel dalam konflik di masa depan. Indonesia telah mempunyai beberapa pertahanan siber. Namun sampai saat ini, Indonesia masih berada dalam tahap proses pengembangan dan penguatan, belum mengarah untuk dapat mengembangkan senjata siber (*cyber-weapon*) yang mampu melakukan serangan balik saat terjadi perang siber. Penelitian ini melakukan analisis trend dan fenomena serangan siber khususnya di Indonesis, serta konseptual pengembangan senjata siber, dan potensi teknologi big data dan artificial intelligence dalam perkembangan senjata otonom di era peperangan siber. Data menunjukkan bahwa trend serangan siber global semakin mengalami peningkatan seiring dengan pengguna internet yang terus meningkat. Untuk memperkuat pertahanan siber, Indonesia perlu untuk mempertimbangkan pengembangan senjata siber. Hasil analisis penelitian ini menyimpulkan bahwa senjata siber perlu untuk dispesifikasikan untuk mengembangkan platform, seperti sistem komando dan kontrol, payload, dan operator terlatih, yang mampu memenuhi kebutuhan pengguna.

Kata kunci: senjata, perang siber, pertahanan

Abstract *- Attacks through cyberspace without having to bring physical force to the military have become a new trend in modern warfare in the 21st century. Through cyber attacks, a country can create widespread damage in its opponents, such as crippling control systems of military equipment and other critical infrastructure systems. Some developed countries have built and prepared cyber defense organizations. These countries already have a modern military prepared to use cyberspace as a parallel battleground in future conflicts. Indonesia already has some cyber defense, however, until now, Indonesia is still in the stage of developing and strengthening processes, not yet leading to developing cyber-weapons capable of counterattacking during cyber warfare. The trends and phenomenon of cyber attacks particularly in Indonesia was reviewed in this research, as well as conceptual development of cyber weapons, and the potential of big data technology and artificial intelligence in the development of autonomous weapons in the era of cyber-warfare. Data showed that the trend of global cyber attacks is significantly increasing as internet users continue to increase. To strengthen cyber defense, Indonesia needs to consider the development of cyber weapons. From this study, it is concluded that the requirement and objectives for cyber weapons need to be specified in order to develop the platforms suitable, e.g. command and control systems, payloads and trained operators that meet for the user needs.*

Keywords: *weapons, cyber-warfare, defense*

[1] Program Studi Teknologi Persenjataan, Fakultas Teknologi Pertahanan, Universitas Pertahanan
[2] Teknologi Penginderaan, Fakultas Teknologi Pertahanan, Universitas Pertahanan

Pendahuluan

Perkembangan lingkungan dan konteks strategis yang dinamis senantiasa membawa perubahan terhadap spektrum ancaman yang kompleks dan berimplikasi terhadap pertahanan negara. Kompleksitas ancaman digolongkan kedalam pola dan jenis ancaman yang multidimensional berupa ancaman militer, ancaman nonmiliter dan ancaman hibrida yang dikategorikan dalam bentuk ancaman nyata dan belum nyata. Wujud ancaman nyata yang dihadapi Indonesia saat ini diantaranya adalah serangan siber,[3] sejalan dengan dunia yang memasuki revolusi industri 4.0 dan era internet of thing (IoT) yang memungkinkan semua terhubung dengan jaringan siber. Panglima TNI menuturkan bahwa perkembangan teknologi tidak hanya membawa nilai positif bagi kehidupan manusia, namun juga memiliki beberapa paradoks yang perlu dicermati, terutama ancaman yang saat ini terus diwaspadai, seperti ancaman siber (*cyber threats*), ancaman biologi (*bio threats*) dan ancaman kesenjangan (*inequality threats*).[4]

Cyber-space atau dalam bahasa Indonesia disebut sebagai dunia maya yaitu sebuah domain operasional yang menggunakan elektro atau elektromagnetik untuk membuat, menyimpan, memodifikasi, serta saling menukar informasi.[5] Jika dahulu penguasaan wilayah sebagai yang utama, maka di era berkembangnya teknologi saat ini, penguasaan lebih bersifat virtual yaitu penguasaan dan pengelolaan terhadap dunia maya yang tersimpan dalam Big Data. Berbeda dengan kedaulatan konvensional negara yang memiliki batasan fisik, kedaulatan siber tidak memiliki batas yurisprudensi yang jelas, tapi harus diamankan untuk menjaga kegiatan strategis negara. Biaya yang rendah dan potensi dampak yang tinggi menjadikan kekuatan cyber menarik bagi semua aktor.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara menyebutkan bahwa pertahanan negara bertujuan untuk menjaga dan melindungi

[3] Kementerian Pertahanan Indonesia, *Buku Putih Pertahanan Indonesia*, (Jakarta: Kemhan RI, 2015), Hlm 1

[4] Marsekal TNI Hadi Tjahjanto. dalam kuliah tamu di Universitas Pertahanan, Sentul, Bogor (13 Maret 2018)

[5] Bryant, Rebecca, *What Kind of Cyber Space*, ISSN 1393-614X Minerva - An Internet Journal of Philosophy 5 (2001): 138–155

kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI) dan keselamatan segenap bangsa dari segala bentuk ancaman, baik ancaman militer maupun non-militer. Ancaman nonmiliter khususnya di ruang siber telah menyebabkan kemampuan negara dalam bidang soft dan smart power pertahanan harus ditingkatkan melalui strategi penangkalan, penindakan dan pemulihan pertahanan siber (*cyber-defense*) dalam rangka mendukung penerapan strategi nasional keamanan siber yang dimotori oleh Kementerian Komunikasi dan Informatika.

Perang dan konflik dalam dunia siber terjadi dalam berbagai bentuk, mulai dari cyber-crime, hingga terorisme. Motif dari cyber-crime bermacam-macam, bisa karena kebencian, mencari keuntungan semata, sampai bermotif moral. Dewasa ini, serangan siber (*cyber-attack*) semakin sering dilakukan pada dan oleh negara. Hal ini membawa *cyber-crime* pada dimensi konflik yang baru, yaitu peperangan siber (*cyber-warfare*) dengan melibatkan negara pada ranah internasional. Peperangan siber disini merupakan pertarungan perang dengan potensi untuk menghancurkan fisik, teknis, dan infrastruktur virtual, serta merusak kemampuan nasional. Dengan melihat dampak dari cyber-war tersebut, diperlukan suatu pertahanan siber (*cyber-defense*) untuk melindungi pertahanan dan keamanan serta keberlangsungan hidup negara.

Meninjau dari pengertian senjata yaitu alat yang digunakan, atau dirancang untuk digunakan dengan tujuan mengancam atau menyebabkan kerusakan fisik, fungsi, atau mental pada struktur, sistem, atau makhluk hidup.[6] Maka siber dapat didefinisikan sebagai senjata (*cyber-weapon*) jika program komputer tersebut dirancang untuk membahayakan integritas atau ketersediaan data dalam sistem IT musuh terutama untuk tujuan militer.[7] Oleh karena itu, senjata siber merupakan kode komputer yang digunakan, atau didesain untuk digunakan dengan tujuan mengancam atau mengacaukan fisik, fungsi, atau kerusakan pada struktur atau sistem infrastruktur kritis, seperti menghentikan sistem email militer, kilang dan pipa minyak meledak, kendali sistem lalu lintas udara terhenti, kereta api

[6] Thomas Rid dan Peter Mc Burney, *Cyber Weapons*, The RUSI Journal 157:1, 6-13, DOI:10.1080/03071847.2012.664354

[7] James M. Acton, *Cyber Weapons and Precision Guided Munitions, Carnegie Endowment For International Peace*, Published 16 October 2017

barang dan metro tergelincir, pembangkit listrik berhenti, bahkan dapat membuat satelit yang mengorbit lepas kontrol.[8] Cyber-weapon ini juga menimbulkan gangguan pada sektor finansial, pemerintahan dan militer, maupun meningkatkan metode terorisme, serta dapat digunakan untuk melumpuhkan perbankan di suatu negara, mengacaukan data, melumpuhkan instalasi dan institusi negara, catatan medis lenyap, dan lainnya.[9] Selain menyebabkan bahaya lethal yang terlihat, cyber-weapon juga memiliki potensi untuk berimplikasi pada kehidupan manusia melalui metode yang tidak langsung, seperti sistem radar penerbangan di bandara yang beberapa kali mengalami gangguan. Senjata ini pada umumnya hadir dalam bentuk malware (malicious software).

Serangan siber telah banyak dilakukan dengan target negara hingga berdampak pada dimensi keamanan internasional. Kemajuan teknologi modern memberikan banyak perubahan dalam seni peperangan, dimana berbagai negara telah menggunakan perangkat lunak sebagai senjata yang cukup kuat untuk melumpuhkan politik, pertahanan dan teknologi. Salah satu virus perangkat lunak mematikan yang diberi nama StuxNet, yaitu cacing komputer 500KB yang menginfeksi banyak pabrik industri di Iran telah menyusup dan menyabot sistem nuklir dengan cara memperlambat ataupun mempercepat motor penggerak reaktor nuklir hingga membuatnya berputar jauh diatas kecepatan maksimum.[10] Tidak seperti virus komputer biasa, Stuxnet dirancang sedemikian rupa sehingga dapat berhasil menyusup kedalam sistem *Supervisory Control And Data Acquisition* (SCADA) dan menyebar dengan cepat dari satu komputer ke komputer lain dengan atau tanpa internet. StuxNet secara tersembunyi menyebar pada komputer yang berjalan di windows bahkan tanpa koneksi internet, hanya dengan melalui drive USB.

Beberapa negara-negara maju di dunia telah membangun dan mempersiapkan organisasi pertahanan

---

[8] Rid and McBurney, *Cyber Weapons*, The RUSI Journal. ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: http://www.tandfonline.com/loi/rusi20

[9] Maloney Sarah, *Cyber Crime Adds A Powerful New Weapon To Terrorists' Arsenal And It's Only A Matter Of Time Before They Deploy It*, Cyberason, 20 April 2017.https://www.cybereason.com/blog/ blog-cyber-crime-adds-a-powerful-new-weapon-to-the-terrorists-arsenal (diakses 23 Juli 2018)

[10] Falliere, Murchu, Chien, *W32. Stuxnet Dossier*, Symantec Security Response. Version 1.4 (February 2011)

siber (*cyber-defense organization*) yakni badan yang bertanggungjawab atas keamanan internet sekaligus mampu menghimpun segala usaha pertahanan dan serangan balik terhadap lawan. Negara-negara tersebut telah memiliki militer modern disiapkan untuk menggunakan dunia maya sebagai medan pertempuran paralel dalam konflik di masa depan, dimana para penyerang akan memiliki akses keperalatan yang paling canggih yang berhubungan dengan pertahanan lawan. Hal ini menandai lahirnya kecenderungan *cyber-warfare* sebagai salah satu cara berperang saat ini. Dimungkinkan perang atau konflik-konflik yang terjadi di dunia pada masa mendatang akan mengurangi penggunaan gencatan senjata secara langsung dan menggunakan cyber-warfare sebagai cara melakukan serangan.

Penelitian ini menggunakan metode kualitatif deskriptif dengan melakukan eksplorasi atau menjelaskan lebih luas permasalahan yang ada serta keterkaitan variabel-variabel penelitian yang digunakan. Adapun fokus penelitian adalah trend serangan siber di Indonesia, anatomi dan konseptual senjata siber (cyber-weapon) dalam meningkatkan pertahanan di era cyber-warfare, serta potensi big data dan teknologi artificial intelligence dalam perkembangan teknologi senjata otonom di era cyber-warfare.

Hasil dan Pembahasan

Trend dan Fenomena Serangan Siber di Indonesia

Revolusi industri keempat saat ini begitu erat hubungannya dengan *Internet of things* (IoT) dimana berbagai alat maupun infrastruktur lebih menekankan kepada integrasi antar alat dengan menggunakan internet dan pemanfaatan big data. Teknologi IoT ini dapat membawa implikasi kepada organisasi hingga pertahanan negara ketika konektivitas tersebut direlasikan dengan infrastruktur kritis nasional seperti jaringan listrik (electrical grid), jaringan transportasi, bahkan alat utama sistem senjata pertahanan negara (alutsista).

Revolusi industri 4.0 juga telah membuat kemajuan penting di bidang militer, terutama dalam Revolution in Millitary Affairs (RMA). RMA secara filosofis merupakan upaya revolusionis mengubah paradigma berperang, tidak hanya dari sisi persenjataan dan teknologi pertahanan, melainkan manajerial organisasi militer berkaitan

dengan pemerintah dan doktrin-doktrin atau cara-cara berperang.

Sejak tahun 1998 hingga saat ini, Indonesia tidak luput dari serangan siber. Berikut adalah beberapa kasus serangan siber yang pernah terjadi di Indonesia.

a. Tahun 1998

Indonesia melakukan perang siber dengan negara lain, terkait dengan masalah politik dan sosial yang terjadi, seperti saat terjadinya kerusuhan rasial.

b. Tahun 1999

Perang siber yang terjadi antara Indonesia dengan Portugal menyangkut kasus Timor Timur, yakni dengan saling serang hingga saling masuk sistem dan mampu menghapus data-data.

c. Tahun 2009

Sejak 2009 hingga beberapa tahun terakhir terjadi perang siber antara Indonesia dengan Malaysia. Aksi saling susup antara hacker ini terjadi ketika muncul konflik politik ataupun persaingan antara Indonesia dengan Malaysia. Meskipun tidak melibatkan pemerintah kedua negara, namun aksi para hacker ini menyerang fasilitas siber milik pemerintah Malaysia maupun Indonesia.

d. Tahun 2010

Pada tanggal 6 Agustus 2010, Symantec sebagai produsen Antivirus Norton, mengumumkan bahwa Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan worm Stuxnet.

e. Tahun 2013

Insiden penyalahgunaan gedung perwakilan diplomatik Australia terhadap penyadapan presiden Indonesia ke-6 dan beberapa pejabat tinggi negara. Penyadapan ini diinformasikan dan disebarluaskan di media internasional oleh mantan matamata Amerika Serikat Edward Snowden yang menyebutkan informasi dokumen rahasia tersebut ke Australian Broadcasting Corporation (ABC).

f. Tahun 2017

Serangan ransomware WannaCrypt atau WannaCry yang melanda di berbagai belahan dunia termasuk di Indonesia pada tahun 2017. Hingga saat ini masih terus diwaspadai. Serangan siber ini menyasar berbagai perusahaan yang memiliki sistem jaringan dengan cara mengubah file di komputer korban menjadi data terenkripsi dan meminta sejumlah uang terbusan untuk kunci deksripsi (untuk menguraikan file dan mengembalikannya menjadi data asli). Setidaknya dua rumah sakit di Jakarta yang disinyalir terserang ransomware berjenis WannaCry pada 12 Mei 2017 yaitu

Dharmais dan Harapan Kita, yang telah menyebabkan data pasien dalam jaringan komputer rumah sakit tidak bisa diakses.

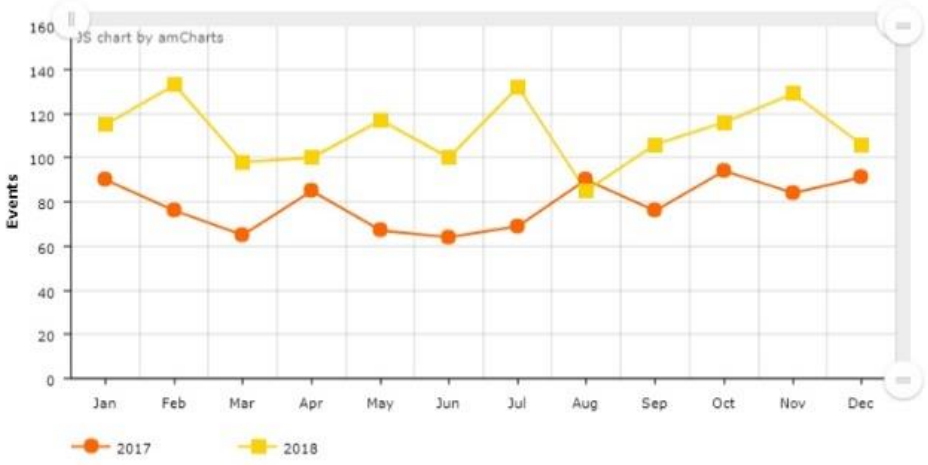
g. Tahun 2018

Perusahaan kemanan siber Kaspersky Labs mencatat terjadi adanya peningkatan signifikan serangan WannaCry terhadap perangakat di berbagai negara. Pada kuartal ketiga 2018, malware tersebut telah menyerang 74.621 pengguna unik di seluruh dunia, dan Indonesia menjadi salah satu negara yang paling banyak mendapatkan serangan malware kripto yakni sebesar 8,8% dari total penyerangan malware kripto.

Berdasarkan fenomena tersebut, *cyber-weapon* bukan hanya berpotensi menjadi *weapon of mass destruction*, namun juga berpotensi menjadi *weapon of mass disruption*. Telah dilakukan berbagai usaha oleh pemerintah, akademisi, dan industri untuk mengantisipasi dan memitigasi serangan siber, seperti pembentukan Badan Siber Sandi Negara (BSSN) yang membidangi siber nasional dan berfungsi menentukan kebijakan keamanan siber nasional dengan peran dan kerjasama antara pemerintah, sektor swasta serta masyarakat. Diprediksi, serangan-serangan siber di dunia termasuk di Indonesia terus berkembang dan mengalami peningkatan.

Beberapa negara-negara maju di dunia telah membangun dan mempersiapkan organisasi pertahanan siber (*cyber-defense organization*) yakni badan yang bertanggungjawab atas keamanan internet sekaligus mampu menghimpun segala usaha pertahanan dan serangan balik terhadap lawan. Negara-negara tersebut telah memiliki militer modern disiapkan untuk menggunakan dunia maya sebagai medan pertempuran paralel dalam konflik di masa depan, dimana para penyerang akan memiliki akses keperalatan yang paling canggih yang berhubungan dengan pertahanan lawan. Hal ini menandai lahirnya kecenderungan cyber-warfare sebagai salah satu cara berperang saat ini. Dimungkinkan perang atau konflik-konflik yang terjadi di dunia pada masa mendatang akan mengurangi penggunaan gencatan senjata secara langsung dan menggunakan cyber-warfare sebagai cara melakukan serangan.

Ancaman dan serangan-serangan siber pun sudah semakin canggih dengan berkembangnya teknologi dan juga taktik pelakunya dalam menerobos pertahanan siber yang ada, karena itu peningkatan



Gambar 1. Bagan Koordinasi, Jejaring Kerja dan Kemitraan Surveilans Kesehatan
Sumber: Permenkes No.45 Tahun 2014

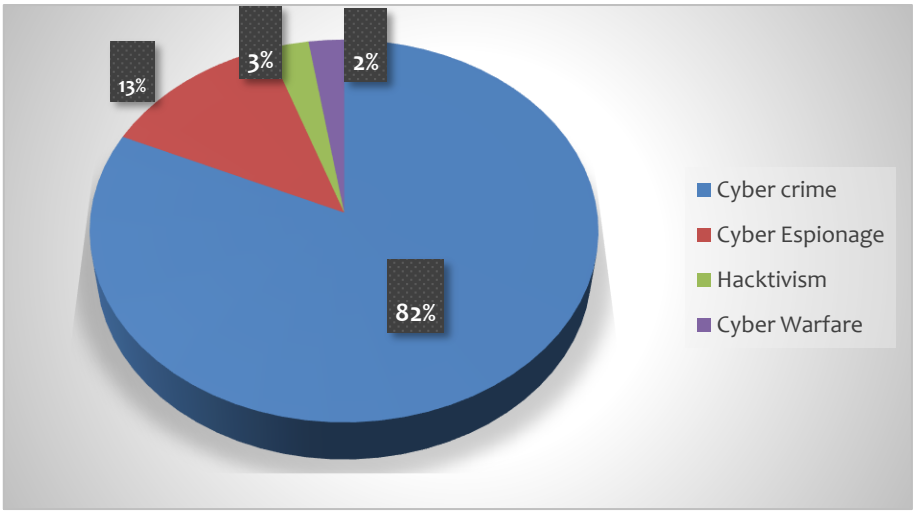
keamanan siber diterapkan bukan pada saat perlu saja atau sebagai cara untuk menangkal ancaman atau serangan siber saja, melainkan sudah merupakan suatu tindakan darurat dan keharusan, mengantisipasi ancaman dan serangan siber yang lebih parah pada pencurian data-data negara, organisasi maupun pribadi.

Berdasarkan serangan siber global yang dirangkum oleh *hackmageddon information security timelines and statistics* menunjukkan bahwa serangan pada pada tahun 2018 lebih tinggi daripada serangan pada tahun 2017, hal ini dikarenakan jumlah pengguna internet terus meningkat. Namun kedua grafik tersebut mengalami fluktuatif.

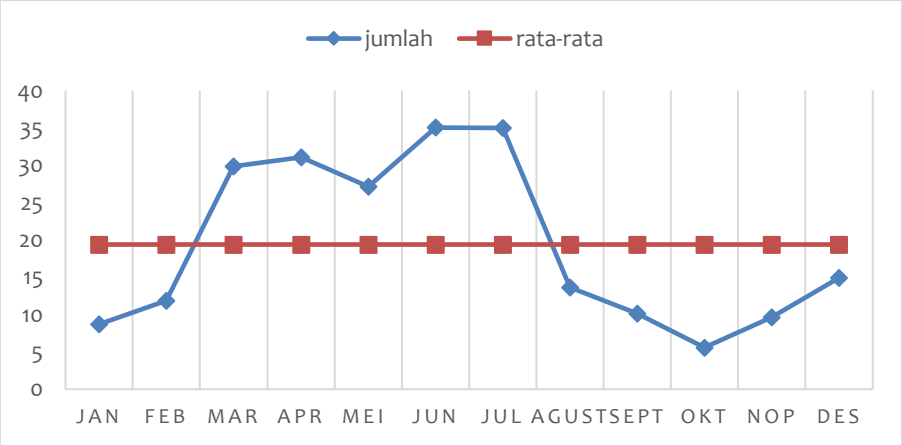
Gambar 2. menunjukkan bahwa mayoritas motivasi dari serangan siber adalah untuk hal criminal atau cyber crime yakni sebesar 81% dari total kasus serangan. Serangan paling banyak menggunakan malware yakni sebanyak 34%, dimana tiga target utama dari serangan siber secara berurutan yaitu menyerang target individu, industri, serta administrasi publik, pertahanan, dan keamanan nasional.

Grafik dari hasil monitoring ID-SIRTII pada tahun 2018 menunjukkan trend serangan siber di Indonesia mengalami fluktuatif tiap bulannya, dimana pada bulan Januari sampai dengan Desember 2018 terjadi serangan siber dengan total 232 juta serangan dengan rata-rata 19 juta serangan per hari. Trend ini diperkirakan akan mengalami peningkatan, seiring dengan pengguna internet yang terus meningkat begitupun dengan internet of things di Indonesia. Trend tersebut menunjukkan bahwa serangan siber merupakan ancaman nyata dan perlu diantisipasi agar tidak berdampak luas.

Serangan Denial Distribute of services atau DDoS Attack merupakan



Gambar 2. Motivations of cyber attack 2018
Sumber: hackmageddon.com, 2018



Gambar 3. Grafik Serangan Siber di Indonesia
Sumber: Diolah dari data Id-Sirtii, 2018

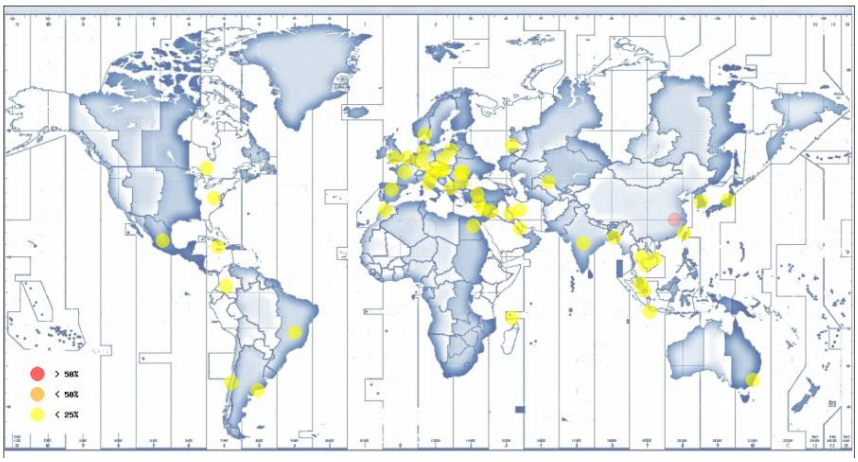
serangan sederhana yang memberikan dampak menghabiskan sumber (resource) yang dimiliki oleh website ataupun server tersebut hingga tidak dapat menjalankan fungsinya dengan benar. Hal ini secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari website ataupun server yang sedang terkena dampak DDoS karena penuhnya lalu lintas kinerja pada server ataupun website.

Berikut adalah skema dari DDoS dari data *threat geolocation* yang terangkum oleh Universitas Pertahanan

Gambar 4. menunjukkan bahwa terdapat banyak ancaman terhadap server universitas pertahanan banyak berasal dari luar negeri, dan terutama serangan terbanyak berasal dari China. Namun terdapat juga serangan yang menggunakan proxy, dimana seolah-olah serangan tersebut berasal dari negara X, kenyataannya dari negara Y.

Konseptual dan Anatomi Senjata Siber di Indonesia

Dalam upaya memperkuat pertahanan siber, Kementerian



Gambar 4. Threat Geolocation
Sumber: Business & Compliance ISO PCI Report 2018

Pertahanan Indonesia dan Tentara Nasional Indonesia telah menerapkan siber militer di lingkungan organisasi masing-masing. Kementerian Pertahanan memiliki Pusat Data dan Informasi (Pusdatin) yang mempunyai tugas melaksanakan pembinaan, pengembangan dan standarisasi teknis di bidang sistem informasi, teknologi informasi, sistem komunikasi data dan persandian pertahanan negara.[11] Salah satu satuan kerja dibawah naungan Pusdatin Kementerian Pertahanan adalah *Cyber Operation Center* yang memiliki tugas mempertahankan infrastruktur vital dan serangan siber, dimana didalamnya terdapat beberapa laboratorium seperti laboratorium monitoring, digital forensic, elektro,jaringan,malwere, dan simulasi.

Di dunia militer, keberadaan tentara siber sudah menjadi kebutuhan, seperti Amerika, Korea Utara, China, Singapura, Australia yang telah memiliki tentara siber. Pada Oktober 2017, TNI meluncurkan satuan siber (satsiber) yang bertujuan untuk melindungi sumberdaya informasi di lingkungan TNI dari gangguan dan penyalahgunaan maupun pemanfaatan oleh pihak-pihak lain.

Dalam meningkatkan keamanan jaringan organisasi, diperlukan pengembangan suatu *konsep Six-Ware Framework* (The SWF) yang dikembangkan oleh Rudy dan Baskoro[12]. Pemberdayaan SWF tidak hanya seperangkat daftar tindakan yang harus dilakukan, tetapi menyajikan solusi keamanan jaringan utama untuk mengelola risiko keamanan dan analisis

[11] Kemhan, *Pusat Data dan Informasi*, https://www.kemhan.go.id/pusdatin/tugas-fungsi

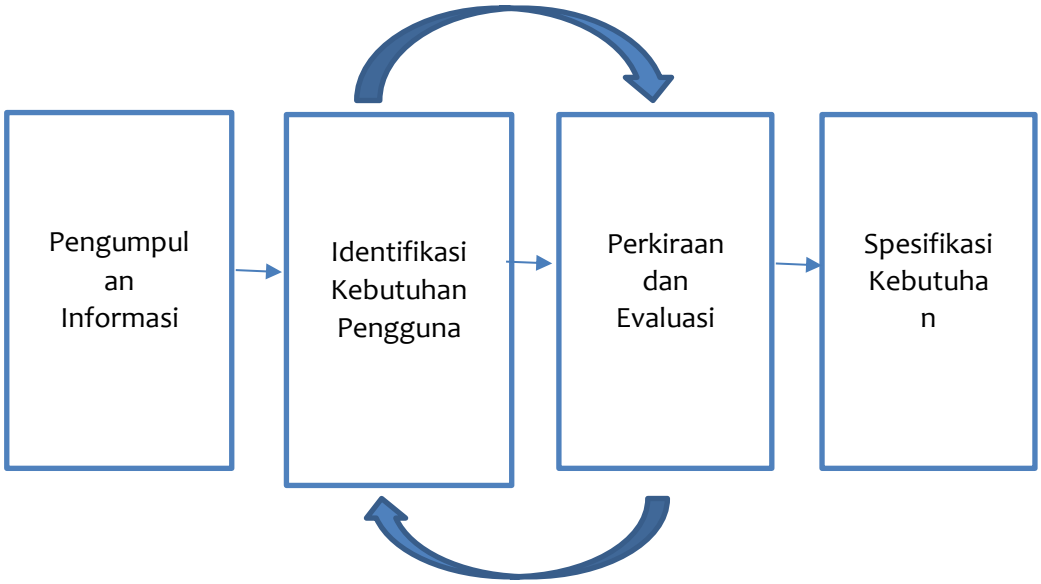
[12] Rudy AG Gultom dan Baskoro Alrianto, *Enhancing Network Security Environment by Empowering Modeling and Simulation Strategy*, ICIMP 2016 : The Eleventh International Conference on Internet Monitoring and Protection

dalam jaringan komputer organisasi. Penggerak SWF terdiri dari enam aspek utama, yaitu

a. *Brainware* atau faktor manusia, adalah aspek utama dalam lingkungan keamanan jaringan.
b. *Hardware* atau perangkat keras, memainkan peran dominan dalam menangani ancaman, serangan, dan kerentanan.
c. *Software* atau perangkat lunak, berkaitan dengan pemanfaatan keamanan aplikasi perangkat lunak yang digunakan setiap hari di kantor, seperti email, situs web, media sosial, dan aplikasi lainnya. Kesadaran keamanan tinggi sangat diperlukan karena penyerang akan selalu berusaha menginfeksi dengan mengirimkan email berbahaya dan lampirannya atau mengundang untuk mengunjungi situs web yang terinfeksi malware.
d. *Infrastructureware,* memiliki peran penting dalam memfasilitasi infrastruktur jaringan organisasi yang aman, mis., Memantau jaringan dari berbagai ancaman, serangan, dan kerentanan.
e. *Firmware*, termasuk dokumentasi strategi dan kebijakan keamanan organisasi, prosedur operasi standar (SOP), rencana kesinambungan bisnis (BCP), kerangka kerja keamanan jaringan atau kepatuhan standardisasi keamanan internasional kepada Organisasi Internasional untuk Standardisasi (ISO), seperti ISO 27001: 2013, Kerangka kerja keamanan cyber NIST versi 1.0 atau kebijakan dan strategi keamanan pemerintah.
f. *Budgetware* atau anggaran, memainkan peran penting dan strategis dalam memfasilitasi implementasi variabel lima-perangkat di atas. Hal ini karena sebuah organisasi didesak untuk menyediakan uang yang cukup besar atau anggaran yang cukup untuk membeli misalnya, alat aplikasi keamanan jaringan, sistem patching, lisensi perangkat lunak, pelatihan dan pendidikan, program sertifikasi, dan lain lain. Sangat disarankan manajemen tingkat atas harus meletakkan masalah ini sebagai prioritas tingkat tinggi untuk membangun kesadaran keamanan informasi. Mengalokasikan anggaran keamanan informasi yang memadai dapat melindungi seluruh sistem jaringan. Jika tidak, mereka akan menghadapi kerugian finansial yang signifikan dari organisasi, dll.

Hasil wawancara dengan Satsiber TNI, Satuan Siber TNI mempunyai tugas pokok melindungi infrastruktur kritis milik TNI. Dalam waktu saat ini karena masih baru dibentuk, jadi konsentrasi satsiber TNI masih dalam tahap menjaga keamanan siber, yakni membangun infrastruktur untuk keamanan siber, belum mengarah untuk menciptakan cyber-weapon yang mampu menyerang balik.

Dari rencana tersebut, meski Indonesia masih berada dalam tahap mengembangkan pertahanan siber (*cyber-defense*) namun Indonesia memiliki rencana jangka panjang untuk dapat mengembangkan senjata yang mampu melakukan serangan siber (*cyber-attack*) yakni dalam wujud senjata siber (*cyber-weapon*). Jika suatu negara dapat mempertimbangkan anggaran biaya yang tidak sedikit untuk pemenuhan kemampuan persenjataan kinetik sebagai alat pertahanan dan keamanan nasional, maka suatu negara juga perlu mempertimbangkan untuk mengembangkan sistem senjata cyber yang memiliki presisi yang serupa dengan senjata kinetik dalam memberikan efek pada target. Dalam beberapa kasus, investasi yang dibutuhkan untuk mengembangkan dan menggunakan kapabilitas siber mungkin lebih kecil daripada kapabilitas kinetik. Dimana jika efek dari sistem senjata cyber bermanfaat dalam pertahanan Indonesia, maka laba atas investasi senjata cyber bisa jadi lebih tinggi dari senjata kinetik.



Gambar 5. Proses Umum dari Analisis Kebutuhan
Sumber: Martin Maguire and Nigel Bevan, "User requirements analysis", 2002

Basis untuk penerapan metode user requirement pada penelitian ini menerapkan teori dari Martin Maguire and Nigel Bevan, "User requirements analysis", 2002.

Setelah dilakukan tahap pengumpulan informasi dan identifikasi kebutuhan pengguna, selanjutnya adalah melakukan tahap perkiraan dan evaluasi, serta spesifikasi kebutuhan. Berikut adalah komponen-komponen senjata cyber, terutama dari segi cost.

a. Platform Pengiriman

Platform senjata cyber memiliki persyaratan yang terbatas untuk menjalani pengujian di lingkungan yang ekstrem.

b. Konstruksi Platform

Beberapa kemampuan senjata cyber membutuhkan pengerasan/hardening dan untuk dapat beroperasi dalam fasilitas "lunak".

c. Pengembangan, pengujian, dan evaluasi efek.

Sistem cyber-weapon harus dilakukan pengujian untuk menilai potensi dari efek yang tidak diinginkan. Pengujian pada umumnya tidak perlu hingga menyebabkan kerusakan fisik, sehingga jangkauannya dapat digunakan secara luas.

d. Persiapan Intelijen

Untuk dapat efektif, senjata cyber membutuhkan intelijen yang sangat tinggi. Jika satu nomor alamat IP salah, maka senjata tidak akan memiliki efek sama sekali. Oleh karena itu, Intelijen yang diperlukan seringkali "berlapis" sehingga beberapa operasi pengumpulan intelijen harus dilakukan sebelum dimulai operasi cyber.

a. Konstruksi dan Pemeliharaan

Semua komponen sistem senjata cyber dapat disimpan. Setelah musuh telah dapat mengembangkan counternya, setiap muatan perangkat lunak masih dapat digunakan kembali dengan mengubahnya agar tetap efektif, atau direkayasa ulang sepenuhnya.

b. Pelatihan Personel

Personel memerlukan pelatihan untuk dapat terkualifikasi, dimana pelatihan dapat dilakukan di ruang kelas pada platform dengan perangkat lunak yang terus diperbarui.

c. Jalur Akses

Sebagian dari jalur akses mungkin perlu direkayasa oleh operator cyber untuk memastikan bahwa senjata tersebut dapat mencapai target.

d. Rekonstruksi target yang dihancurkan

Sebagian besar target akan mengalami kerusakan fisik.

Singkatnya, spesifikasi dari kebutuhan (*requirement specification*) senjata cyber yang terdiri dari beberapa platform, yakni sistem komando dan kontrol, payload, dan operator terlatih. Efek awal dari sistem senjata cyber yang presisi mungkin terbatas, tetapi investasi tersebut dapat mengarah pada keefektifan tempur yang signifikan dimana akan meningkatkan pengembalian investasi seiring dengan kemampuan yang semakin matang. Oleh karena itu, pembuat kebijakan perlu kiranya mempertimbangkan untuk mengembangkan sistem senjata cyber yang dalam rangka meningkatkan pertahanan Indonesia di era *cyber-warfare.* Berikut adalah beberapa pertimbangan mengapa Indonesia perlu untuk mengembangkan senjata cyber.

a. Dari segi etis,

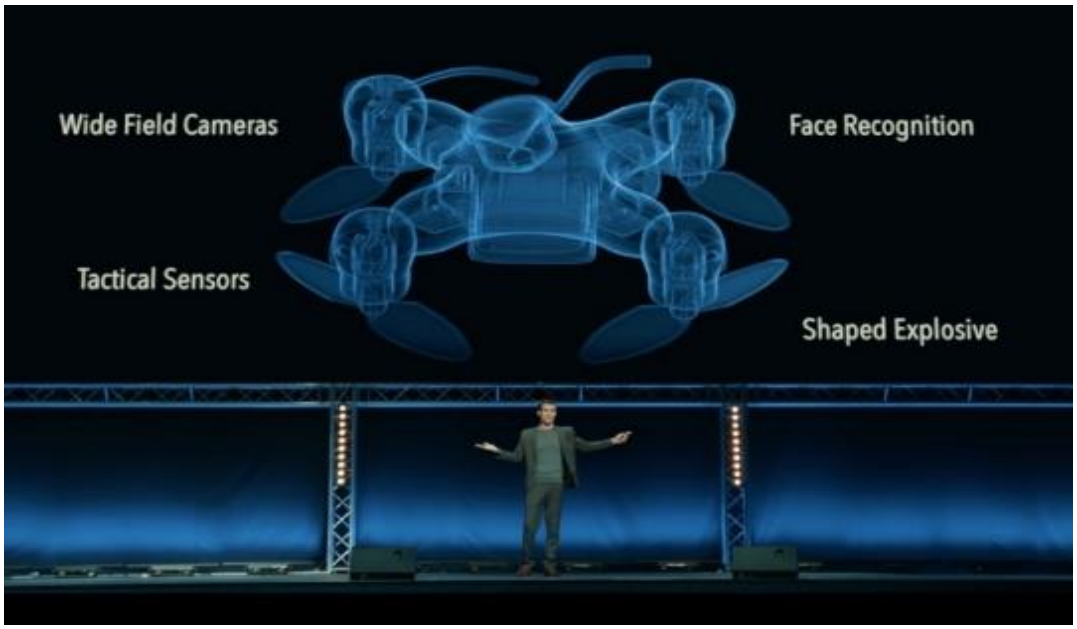
Dalam suatu pertempuran, penggunaan sistem senjata cyber yang presisi dapat mengurangi risiko bahaya dari operator cyber, para kombatan, maupun masyarakat sipil.

b. Dari segi operasional,

Penggunaan senjata cyber dapat membantu para komandan militer untuk mengerahkan pasukannya menjalankan operasi dengan lebih efisien.

c. Dari segi finansial

Potensi penggunaan senjata siber dibandingkan dengan senjata kinetik dapat mengurangi biaya penyimpanan



Gambar 6. Cuplikan Video Fiksi Slaughterbots
Sumber: futureoflife.org, 2018

dan pemeliharaan, dan mengurangi biaya rekonstruksi target.

Potensi *Big Data* dan *Artificial Intelligence* Dalam Perkembangan Senjata Otonom di Era *Cyber-Warfare*

Memasuki era revolusi industri 4.0, jika kemajuan teknologi disalahgunakan, maka tidak menutup kemungkinan dapat dimanfaatkan dalam pengembangan senjata otonom untuk menghancurkan target. Selain perlu mewaspadai serangan siber melalui malware, hal yang juga perlu diwaspadai adalah serangan siber melalui penyalahgunaan perkembangan teknologi *artificial intelligence* (AI) atau kecerdasan buatan. Teknologi AI dapat dimodifikasi agar terhubung oleh *big data* yang berisikan akumulasi data-data identitas seseorang yang beredar di media sosial, untuk mencari dan menyasar seseorang yang menjadi target. Teknologi ini adalah cikal bakal perkembangan teknologi persenjataan otonom, seperti pada Gambar 6. cuplikan video slaughterbots.

Future of Life Institute yang merupakan organisasi pengawas perkembangan kecerdasan buatan pada tanggal 17 November 2017, telah membuat robot imajinasinya sendiri dalam sebuah video fiksi. Robot imajinasi tersebut diberi nama dengan "SlaughterBots" atau robot pembantai yang dapat membunuh secara otonom. Robot drone kecil tersebut bisa membantai manusia dengan cukup sadis karena bahan peledak yang digunakan untuk melubangi tengkorak dan menghancurkan isi otak. Juga dilengkapi dengan berbagai teknologi canggih, serta kamera dan pengenalan wajah seperti pada aplikasi media sosial yang digunakan untuk membuat keputusan tentang target yang akan dibunuh secara otonom.

Tujuan dari video fiksi tersebut adalah untuk meningkatkan kesadaran tentang bahaya senjata robot otonom. Sampai saat ini masih belum ada drone seperti yang tergambar dalam video tersebut.

Dunia teknologi persenjataan hingga saat ini masih bergantung pada manusia untuk menarik pelatuknya dan memutuskan apakah orang yang muncul saat dibidik akan dibunuh atau tidak. Namun tidak mustahil bahwa sistem ini akan semakin otomatis ke titik di mana robot itu sendiri yang akan mengambil keputusan, yakni robot yang dapat membunuh seseorang hanya dengan memasukkan data orang yang akan dibunuh dan dalam prosesnya tidak dikendalikan oleh manusia.

Kesimpulan

Adapun kesimpulan yang diperoleh pada penelitian ini adalah sebagai berikut:

1. Trend serangan siber di Indonesia yang menjadi ancaman keamanan dan pertahanan Indonesia.

Trend serangan siber global semakin mengalami peningkatan seiring dengan pengguna internet yang terus meningkat. Motivasi dari kasus serangan siber paling banyak berasal dari faktor kriminal atau *cyber crime* yakni sebesar 81% dari total kasus serangan, dengan target terbanyak menyerang individu, selanjutnya diikuti oleh industri, administrasi publik, dan pertahanan keamanan nasional.

Begitupun di Indonesia, data Id-Sirtii/CC menunjukkan trend serangan siber di Indonesia mengalami peningkatan secara berkala. Hal ini sejalan dengan pengguna internet di Indonesia yang terus meningkat, dimana Indonesia menduduki peringkat ke-5 pengguna internet tertinggi di dunia. Namun hal ini tak sejalan dengan peringkat indeks keamanan siber di Indonesia yang masih berada di peringkat ke-70 di Asia.

2. Konseptual dan anatomi senjata siber (*cyber-weapon*) dalam meningkatkan pertahanan di era *cyber-warfare*.

Spesifikasi kebutuhan (*requirement specification*) senjata cyber terdiri dari beberapa platform, yakni sistem komando dan kontrol, payload, dan operator terlatih, menunjukkan bahwa sistem senjata cyber dapat memberikan keefektifan yang signifikan, baik dari segi tempur, maupun dalam hal investasi Beberapa pertimbangan Indonesia perlu untuk mengembangkan senjata cyber, yakni dari segi etis, segi operasional, dan segi finansial yang dapat mengurangi biaya dalam penyimpanan dan pemeliharaan, dan mengurangi biaya rekonstruksi target, jika dibandingkan senjata kinetik.

3. Potensi *big data* dan teknologi *artificial intelligence* dalam perkembangan teknologi senjata otonom di era *cyber-warfare*.

Selain perlu mewaspadai serangan siber melalui malware, hal yang juga perlu diwaspadai adalah serangan siber melalui penyalahgunaan perkembangan teknologi *artificial intelligence* (AI) atau kecerdasan buatan. Teknologi AI dapat dimodifikasi agar terhubung oleh *big data* yang berisikan akumulasi data-data identitas seseorang yang beredar di media sosial, untuk mencari dan

menyasar seseorang yang menjadi target. Teknologi ini adalah cikal bakal perkembangan teknologi persenjataan otonom.

Saran

1. Saran Teoritis

Penelitian ini belum mencantumkan hambatan, dan strategi dalam pengembangan senjata cyber, serta spesifikasi teknologi dari senjata cyber yang sesuai untuk diterapkan di Indonesia. Oleh karena itu perlu dilakukan penelitian lebih lanjut untuk menjelaskan mengenai hal-hal tersebut.

2. Saran Praktis

Salah satu faktor penting yang perlu dipertimbangkan dalam pengembangan senjata cyber adalah faktor sumber daya manusia (SDM) Indonesia yang handal terutama di bidang IT. Sehingga diperlukan dukungan dan kerjasama dari organisasi pertahanan siber Indonesia dengan komponen bangsa yang ahli di bidang hacker.

Untuk pembuat kebijakan, selain perlu untuk disahkannya undang-undang perlindungan data pribadi, perlu juga kiranya untuk mempertimbangkan pengembangan sistem senjata cyber dalam rangka meningkatkan pertahanan Indonesia di era cyber-warfare, terutama memaksimalkan potensi badan usaha milik negara industri pertahanan (BUMNIP) untuk turut andil dalam pengembangan senjata cyber. Mempertimbangkan senjata cyber ini berbeda senjata kinetik yang dapat diimpor dari negara luar, senjata cyber harus dikembangkan oleh para ahli-ahli IT di Indonesia. Sehingga dengan adanya pengembangan senjata cyber, Indonesia tidak hanya mampu memperkuat pertahanan siber defensif, namun juga kuat dalam pertahanan siber ofensif.

Daftar Pustaka

Buku

Kementerian Pertahanan Indonesia. 2015. *Buku Putih Pertahanan Indonesia*. Jakarta: Kemhan RI.

Kementerian Pertahanan Indonesia. 2015. *Pedoman Pertahanan Siber*. Jakarta: Kemhan RI, 2014.

Universitas Pertahanan. 2014. *Kajian Strategis Keamanan Cyber Nasional*. Universitas Pertahanan.

Jurnal

Bryant, Rebecca. 2001. "*What Kind of Cyber Space*". ISSN 1393-614X Minerva - An Internet Journal of Philosophy 5 (2001): 138–155

Gultom, Rudy AG dan Baskoro Alrianto. 2016. "*Enhancing Network Security Environment by Empowering Modeling and Simulation Strategy*". ICIMP 2016: The Eleventh International Conference on Internet Monitoring and Protection.

Maguire, Martin dan Nigel Bevan. 2002. "*User requirements analysis: A review of supporting methods*". Proceedings of IFIP 17th World Computer Congress, Montreal, Canada. Kluwer Academic Publishers

Rid, Thomas dan Peter Mc Burney. 2015. "*Cyber Weapons*", The RUSI Journal 157:1, 6-13, DOI: 10.1080/ 03071847. 2012.664354

Internet

Agregasi Antara. 2017. "Kasus Serangan Siber Terheboh di 2017, Apa Saja?", https://techno.okezone.com/read/2017/12/31/207/1838109/kasus-serangan-siber-terheboh-di-2017-apa-saja

Sarah, Maloney. 2017."" *Cyber Crime Adds A Powerful New Weapon To Terrorists' Arsenal And It's Only A Matter Of Time Before They Deploy It". Cyberason, 20 April 2017.https://www.cybereason.com/blog/ blog-cyber-crime-adds-a-powerful-new-weapon-to-the-terrorists-arsenal (diakses 23 Juli 2018)*

NATO. 2018. NATO Review Magazines (online). https://www.nato.int/ , diakses tanggal 19 Juli 2018

Tirto.id, "Panglima TNI: Alutsista Akan Didorong Berbasis Digital dan Big Data", dalam https://tirto.id/panglima-tni-alutsista-akan-didorong-berbasis-digital-dan-big-data-cTck.

Undang-Undang

Keputusan Panglima Tentara Nasional Indonesia Nomor Kep/555/VI/2018 2018 Tentang Doktrin Tentara Nasional Indonesia Tri Dharma Eka Karma

Undang-Undang Nomor 3 Tahun 2002.

Kuliah Tamu

Marsekal TNI Hadi Tjahjanto. 2018. "Ancaman Era Revolusi Industri 4.0". Kuliah tamu di Universitas Pertahanan, Sentul, Bogor (13 Maret 2018)

Wawancara

Lumanto, Rudi. 2018."Interview of Serangan Siber di Indonesia". Kantor BSSN.

Tofik Tofana. 2018. "Peran dan strategi satuan siber TNI dalam era cyber warfare. Mabes TNI